Selected Solutions to Lang's *Algebra*

Swayam Chube

May 6, 2025

Contents

§V Algebraic Extensions

Exercise V.28. ***Part 1.*** Let $f(X_1,\dots,X_n)$ be a homogeneous polynomial of degree 2 over k, i.e., a quadratic form. Suppose f is *anisotropic* over k, i.e., the only non-trivial zero of f over k is the vector $(0,\dots,0)$. Let K/k be an extension of odd degree. Using induction on the degree we shall show that f is anisotropic when viewed as a quadratic form over K. In literature, this is a theorem attributed to Springer.

Throughout, we shall fix an algebraic closure k^a of k and consider all extensions to be embedded inside k^a/k. The base case $K = k$ is clear. Suppose now that $[K:k] \geqslant 3$ and that the hypothesis has been proven for all odd degrees less than $[K:k]$. If the extension K/k admits a proper intermediate field, say L, then due to the inductive hypothesis, f is anisotropic when viewed over L and then again due to the inductive hypothesis, f is anisotropic when viewed over K. Suppose henceforth that K/k admits no proper intermediate fields. In particular, due to the Primitive Element Theorem, this means that the extension K/k is simple, i.e., there exists $\alpha \in K$ such that $K = k(\alpha)$.

Let $d = [K:k] \geqslant 3$ and let $p(X)$ be the minimal polynomial of α over k. Suppose f is not anisotropic over K, which means that there is a non-zero vector in K^n on which f vanishes. Thus, there exist polynomials $g_1,\dots,g_n \in k[T]$ such that $\deg g_i \leqslant d-1$ for $1 \leqslant i \leqslant n$ and

$$f(g_1(\alpha),\dots,g_n(\alpha)) = 0.$$

Consider the polynomial

$$h(T) = f(g_1(T),\dots,g_n(T)).$$

Since $k[T]$ is a PID, we can further impose the condition that $(g_1(T),\dots,g_n(T)) = (1)$. Indeed, if their gcd is some polynomial $g(T)$, then $g(\alpha) \neq 0$, and hence, dividing all the g_i's by $g(T)$, we obtain the desired tuple.

Let $M = \max \deg g_i \leqslant d-1$. The coefficient of T^{2M} on the left hand side is $f(a_{1m},\dots,a_{nm})$ where a_{im} is the coefficient of T^m in $g_i(T)$. Since the vector $(a_{1m},\dots,a_{nm})$ is not identically zero, and f is anisotropic over k, it is clear that $\deg h(T) = 2M \leqslant 2d-2$.

Next, since $h(\alpha) = 0$, we can write $h(T) = p(T)q(T)$ for some polynomial $q(T) \in k[T]$. Note that $\deg q = 2M - d \leqslant d-2$ and is an odd number. As a result, q has an irreducible factor $\widetilde{q}$ of odd degree, and let $\beta \in k^a$ be a root of $\widetilde{q}$. Due to the inductive hypothesis and the fact that $h(\beta) = 0$, we must have that $g_1(\beta) = \cdots = g_n(\beta) = 0$, and hence, $\widetilde{q}$ divides $g_1,\dots,g_n$ in $k[T]$, which is absurd. Thus f is anisotropic over K.

Part 2. Let $f(X_1,\dots,X_n)$ be a homogeneous polynomial of degree 3 over k and K/k a quadratic extension. Note that $K = k(\alpha)$ for any $\alpha \in K \setminus k$. Let $p(T) \in k[T]$ be the minimal polynomial of α over k. This is clearly a quadratic polynomial. Suppose f were isotropic over K, then one can find linear polynomials $g_1,\dots,g_n \in k[T]$ such that

$$f(g_1(\alpha),\dots,g_n(\alpha)) = 0.$$

As in Part 1, since $k[T]$ is a PID, we can further impose the condition that $(g_1(T),\ldots,g_n(T)) = (1)$. Let

$$h(T) = f(g_1(T),\ldots,g_n(T)) \in k[T].$$

Again, since f is anisotropic over k, just as argued in Part 1, it follows that $h(T)$ is a cubic polynomial in $k[T]$. Note that $h(\alpha) = 0$, and thus $h(T) = Ap(T)(T-\beta)$ for some $A, \beta \in k$. It follows that $h(\beta) = 0$, i.e., $g_i(\beta) = 0$ for all $1 \leqslant i \leqslant n$. But this is absurd, since $T - \beta$ cannot divide all the g_i's simultaneously. Thus f is anisotropic over K, as desired.

§VI Galois Theory

Exercise VI.21. (a) Suppose $p \mid \Phi_n(a)$. That is, $\overline{a} \in \mathbb{F}_p$ is a root of $\overline{\Phi}_n(X) \in \mathbb{F}_p[X]$. Note that in $\mathbb{F}_p[X]$,

$$X^n - \overline{1} = \prod_{d \mid n} \overline{\Phi}_d(X).$$

Thus, $\overline{a}^n = 1$ in $\mathbb{F}_p$. Let m be the order of $\overline{a} \in \mathbb{F}_p^\times$. Clearly $m \mid n$. Suppose $m < n$. Because

$$X^m - \overline{1} = \prod_{d \mid m} \overline{\Phi}_d(X).$$

As a result, there is some $d \mid m < n$ with $\overline{\Phi}_d(\overline{a}) = 0$. It follows that $X^n - \overline{1} \in \mathbb{F}_p[X]$ is not separable, a contradiction, since its derivative nX^{n-1} is non-zero in $\mathbb{F}_p[X]$, and thus it shares no roots with $X^n - \overline{1}$.

Conversely, suppose $\overline{a}$ has order n in $\mathbb{F}_p^\times$. Since $X^n - \overline{1} \in \mathbb{F}_p[X]$ is separable, there is a unique $d \mid n$ such that $\overline{a}$ is a root of $\overline{\Phi}_d(X) \in \mathbb{F}_p[X]$. Thus $\overline{a}$ is a root of $X^d - \overline{1}$, whence it follows that $d = n$, as desired.

(b) If p divides $\Phi_n(a)$, then $\overline{a}$ has order n in $\mathbb{F}_p^\times$, whence, due to Lagrange's theorem, $n \mid p-1$. On the other hand, if $p \equiv 1 \pmod{n}$, then from the fact that $\mathbb{F}_p^\times$ is cyclic of order $p-1$, it follows that there exists some $\overline{a} \in \mathbb{F}_p^\times$ having period n, and due to part (a), we know that $p \mid \Phi_n(a)$.

Let $p_1 < p_2 < \cdots < p_k$ be primes $\equiv 1 \pmod{n}$. Set $N = p_1 \cdots p_k n$. If $k = 0$, then set $N = n$. For a sufficiently large positive integer $a \gg 0$, we would have $\Phi_n(aN) > 2$, and hence, has a prime divisor p. Clearly $p \neq p_i$ for $1 \leqslant i \leqslant k$, and $p \nmid n$, so that $p \equiv 1 \pmod{n}$, thereby proving the infinitude of such primes.

Exercise VI.22. Following the hint in the book, we first show that for each prime q and positive integer $r \geqslant 1$, there exists a prime $\ell \neq p$ such that the order of p in $(\mathbb{Z}/\ell\mathbb{Z})^\times$ is q^r. Indeed, consider the fraction

$$b = \frac{p^{q^r} - 1}{p^{q^{r-1}} - 1} = \frac{\left(p^{q^{r-1}} - 1 + 1\right)^q - 1}{p^{q^{r-1}} - 1} = \sum_{i=0}^{q-1} \binom{q}{i+1} \left(p^{q^{r-1}} - 1\right)^i. \tag{$\star$}$$

Let ℓ be a prime dividing b. If ℓ does not divide $p^{q^{r-1}} - 1$, then it is clear that the order of p modulo ℓ is q^r. On the other hand, if ℓ divides $p^{q^{r-1}} - 1$, then from the right hand side of ($\star$) it is clear that ℓ must divide q, i.e., $\ell = q$. Again from the right hand side of ($\star$), it follows that b/q is not divisible by q and is greater than 1. Thus, there is some prime $\ell \neq q$ dividing b. Since this ℓ cannot divide $p^{q^{r-1}} - 1$, the order of p modulo ℓ must be q^r, as desired.

Next, consider the extension $F(\zeta_\ell)/F$. This is an extension of finite fields and hence, is Galois. Let G denote its Galois group. It is known that G is generated by the Frobenius map $\varphi\colon x \mapsto x^p$. Thus, the orbit of ζ_ℓ is

$$\zeta_\ell \mapsto \zeta_\ell^p \mapsto \zeta_\ell^{p^2} \mapsto \cdots.$$

The size of this orbit determines the size of the Galois group, and hence, the degree of the extension. But it is clear from the above orbit that the size of this Galois group is precisely the order of p modulo ℓ, which is q^r by construction.

Thus, we have shown that K/F contains fields of arbitrary prime power degree over F. Finally, using the fact that the compositum of fields having coprime degrees over F has the product degree over F, it follows that K/F contains fields of arbitrary degree over F, whence $K = \overline{\mathbb{F}}_p$, thereby completing the proof.

Exercise VI.23. (a) The standard way to do this is to first write

$$G \cong \bigoplus_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z},$$

where $n_i \geqslant 2$. Using either Dirichlet's theorem on primes in AP or Exercise VI.21(b), choose primes $p_i \equiv 1 \pmod{n_i}$. Set $N = \prod_{i=1}^{r} p_i$ and note that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times \cong \bigoplus_{i=1}^{r} \mathbb{Z}/(p_i-1)\mathbb{Z}.$$

Since G is a quotient of the above group, it is clear that G can be realized as a Galois group over $\mathbb{Q}$.

(b) Again, begin by writing

$$G \cong \bigoplus_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}.$$

Using either Dirichlet's theorem on primes in AP or Exercise VI.21, for each positive integer $i \geqslant 1$, choose a tuple of primes $(p_{i1}, \ldots, p_{ir})$ such that $p_{ij} \equiv 1 \pmod{n_j}$. Further, setting $N_i = \prod_{j=1}^{r} p_{ij}$, we may further impose the condition that $\gcd(N_i, N_j) = 1$ whenever $i \neq j$. In particular, this means that $\mathbb{Q}(\zeta_{N_i}) \cap \mathbb{Q}(\zeta_{N_j}) = \mathbb{Q}$. As in part (a), we can find a subfield $E_i \subseteq \mathbb{Q}(\zeta_{N_i})$ such that $\mathrm{Gal}(E_i/\mathbb{Q}) \cong G$.

$$\begin{tikzcd}
 & kE_i & \\
k \arrow[ur, dash] & & E_i \arrow[ul, dash] \\
 & k \cap E_i \arrow[ul, dash] \arrow[ur, dash] & \\
 & \mathbb{Q} \arrow[u, dash] &
\end{tikzcd}$$

We know that $\mathrm{Gal}(kE_i/k) \cong \mathrm{Gal}(E_i/k \cap E_i)$ for all $i \geqslant 1$. We contend that $k \cap E_i = \mathbb{Q}$ for infinitely many $i \geqslant 1$. Indeed, since $k/\mathbb{Q}$ is separable, due to the Primitive Element Theorem, there are only finitely many intermediate fields in the extension $k/\mathbb{Q}$. Thus, there is an infinite subset $I \subseteq \mathbb{N}$ such that $k \cap E_i = k \cap E_j$ for all $i, j \in I$. Then, for $i, j \in I$, we have

$$k \cap E_i = (k \cap E_i) \cap (k \cap E_i) = k \cap (E_i \cap E_j) = k \cap \mathbb{Q} = \mathbb{Q}.$$

Thus, $\mathrm{Gal}(kE_i/k) \cong \mathrm{Gal}(E_i/\mathbb{Q}) \cong G$.

All that remains to be shown is that the set $\{kE_i : i \in I\}$ is infinite. Suppose not, then there is an extension F/k and an infinite subset $J \subseteq I$ such that $kE_j = F$ for all $j \in J$. In particular, $E_j \subseteq F$ for all $j \in J$. Note that $F/\mathbb{Q}$ is a finite separable extension, and hence, due to the Primitive Element Theorem, has at most finitely many intermediate fields, but this is absurd, since $E_i \neq E_j$ for $i, j \in J$. Thus, the set $\{kE_i : i \in I\}$ is infinite, as desired.

Exercise VI.25. First note that every finite extension of k is Galois, and hence k is perfect. Further, since any algebraic extension of k is a union of finite subextensions (each of which is Galois), we have that every algebraic extension of k is Galois so we can freely talk about its Galois group. Finally, we make note of the fact that k can have at most one finite extension of a given degree in k^a. Indeed, if E and F are two finite extensions of k in k^a of the same degree, then $\mathrm{Gal}(EF/E)$ and $\mathrm{Gal}(EF/F)$ are subgroups of $\mathrm{Gal}(EF/k)$ of the same order. Since $\mathrm{Gal}(EF/k)$ is cyclic, it has at most one subgroup of a given order, and hence, $\mathrm{Gal}(EF/E) = \mathrm{Gal}(EF/F)$, i.e., $E = F$.

Let

$$\Sigma := \{(E,\sigma_E)\colon k \subseteq E \subseteq k^a \text{ and } \sigma_E \in \mathrm{Gal}(E/k) \text{ such that } E^{\sigma_E} = k\}.$$

This is clearly a poset under the relation $(F,\sigma_F) \leqq (E,\sigma_E)$ if and only if $F \subseteq E$ and $\sigma_E|_F = \sigma_F$. Clearly, Zorn's lemma is applicable and let (M,σ_M) be a maximal element in Σ. We contend that $M = k^a$.

Suppose $M \subsetneq k^a$ and choose an element $\alpha \in k^a \setminus M$ of minimum degree over M. Since $M(\alpha)/k$ is Galois, we can extend σ_M to an automorphism $\sigma_1 \in \mathrm{Gal}(M(\alpha)/k)$. The maximality of (M,σ_M) implies the existence of some $\beta \in M(\alpha) \setminus M$ which is fixed by σ_1. Note that the minimality of the degree of α over M further implies that $M(\alpha) = M(\beta)$.

$$\begin{tikzcd}
& M(\alpha)=M(\beta) \arrow[dl, dash] \arrow[dr, dash] & \\
M \arrow[dr, dash] & & k(\beta) \arrow[dl, dash] \\
& k &
\end{tikzcd}$$

We contend that $[M(\beta):M] = [k(\beta):k]$. Indeed, let $f(X) = \mathrm{Irr}(\beta,M,X)$ be the irreducible polynomial of β over M. Since σ_1 fixes β, we see that β is a root of $f^{\sigma_1} \in M[X]$. Again, since $\deg f = \deg f^{\sigma_1}$, it follows that $f = f^{\sigma_1}$. In particular, the coefficients of f lie in the fixed field $M^{\sigma_1} = M^{\sigma_M} = k$. Thus, $f(X) = \mathrm{Irr}(\beta,k,X)$, so that $[k(\beta):k] = [M(\beta):M]$.

Now note that $f(X)$ is a separable polynomial and has degree at least 2. Let $\beta' \neq \beta$ be another root of $f(X)$ in k^a and extend the automorphism σ_M to an automorphism σ_2 of $M(\beta)$ sending $\beta \mapsto \beta'$. Again, due to maximality, σ_2 must fix some $\gamma \in M(\beta) \setminus M$. Furthermore, as we argued above, we must have $M(\beta) = M(\gamma)$ and $[k(\gamma):k] = [M(\gamma):M] = [M(\beta):M] = [k(\beta):k]$.

Note that we cannot have $k(\beta) = k(\gamma)$, else $\beta \in k(\gamma)$ would be fixed by σ_2, which is absurd, since $\sigma_2\beta = \beta'$. Thus, $k(\beta)$ and $k(\gamma)$ are distinct Galois extensions of k having the same degree, a contradiction. In conclusion, $M = k^a$, and we have our desired automorphism in $\mathrm{Gal}(k^a/k)$.

Exercise VI.26. Let $\alpha \in \mathbb{Q}^a \setminus \mathbb{Q}$ be an algebraic irrational and E a maximal subfield of $\mathbb{Q}^a$ not containing α. We shall show that every finite extension of E contained in $\mathbb{Q}^a$ is cyclic. Since every finite extension of E is contained in a finite Galois extension, and quotients of cyclic groups are cyclic, it suffices to show that every finite Galois extension of E is cyclic.

Let K be a finite Galois extension of E contained in $\mathbb{Q}^a$ and let $G = \mathrm{Gal}(K/E)$. If F is an intermediate field properly containing E, then it must contain α due to maximality of E, i.e., $E(\alpha) \subseteq F$. Let $H = \mathrm{Gal}(K/E(\alpha))$. From the Galois correspondence, it is clear that H is *the* unique maximal subgroup of G. We shall be done by proving the following:

Claim. Let G be a finite group. If G admits a unique maximal subgroup H, then G is cyclic.[1]

To see this, let $a \in G \setminus H$. If $G \neq \langle a \rangle$, then $\langle a \rangle$ is contained in a maximal subgroup M of G. But since H is the unique maximal subgroup of G, we must have $M = H$, that is, $a \in H$, a contradiction. Thus $G = \langle a \rangle$, as desired.

Exercise VI.27.

Exercise VI.34. Consider two automorphisms $\sigma\colon x \mapsto -x$ and $\tau\colon x \mapsto 1-x$ of $K := \mathbb{C}(X)$ over $\mathbb{C}$. Let E and F denote the fixed fields of σ and τ respectively. Since both σ and τ are order 2 automorphisms, we have that $[K:E] = [K:F] = 2$. Let $k = E \cap F$. Note that k is invariant under the action of $\varphi = \tau \circ \sigma\colon x \mapsto 1+x$. It is clear that φ is an infinite order automorphism of K and that k is contained in the fixed field K^φ. Finally, since K is finite degree over any intermediate field properly containing $\mathbb{C}$, it follows that the fixed field $K^\varphi = \mathbb{C}$. Hence, $k = \mathbb{C}$, so that K is not algebraic over k.

[1] We can further say that G must be a p-group. This follows immediately from the fact that it has a *unique* maximal subgroup.